JCWSCS 0 8 JUN 2004

FILE COPY

QUALCOMM INCORPORATED

5775 Morehouse Drive
San Diego, CA 92121
Fax: (858) 658-2502

Facsimile Transmittal

DATE: June 7, 2004

TO: United States Patent and Trademark Office

ATTN: Office of Initial Patent Examination's Filing Receipt Corrections

FROM: Stacy Dumrauf

FAX NUMBER: (703) 746-9195

Number of Pages Sent: 4 (including this transmittal cover sheet)

Re: U.S. Serial No. 10/762,857
Our Docket No. PA744C2

Dear Sir or Madam:

To follow, please find a Request for Correction of Official Filing Receipt.

Thank you for your assistance. If you have any questions, please contact me at (858) 658-5212.

Stacy Dumrauf

Attorney Docket No. PA744C2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of	)	**For: METHOD FOR NEGOTIATING WEAKENED KEYS IN ENCRYPTION SYSTEMS**
Gregory G. Rose	)	
Serial No. 10/762,857	)	
Filed: January 21, 2004	)	**Group No. 2132**

REQUEST FOR CORRECTION OF OFFICIAL FILING RECEIPT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attn: OFFICE OF INITIAL PATENT EXAMINATION'S FILING RECEIPT CORRECTIONS

Dear Sir:

In response to the Response to Request for Corrected Filing Receipt dated May 21, 2004, please amend the first page of the specification of the above-identified application as follows:

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Depositor's Name: _____
(type or print name)

Date: June 7, 2004

FACSIMILE

☒ transmitted by facsimile to the Patent and Trademark Office.

Depositor's Name: Stacy Dumrauf
(type or print name)

Signature: Stacy Dumrauf

Attorney Docket No. PA744C2

IN THE SPECIFICATION

Please amend the first paragraph of the specification as follows:

This application is a continuation of U.S. Application Serial No. 10/389,364, filed on March 14, 2003, which is a continuation ~~and claims the benefit~~ of U.S. Patent Application Serial No. 09/216,348, filed December 18, 1998, which are incorporated herein by reference in their entirety.

REMARKS

Specification

Applicant provides herewith an amendment to the specification. The amendment to the specification is made by presenting marked up replacement paragraphs which identify changes made relative to the immediate prior version. Attached is the amended first page of the specification.

The changes made are primarily typographical or grammatical in nature, or involve minor clarifications of awkward wordings.

Applicant respectfully requests that a new Official Filing Receipt be issued to Applicant.

Respectfully submitted,

Dated: June 7, 2004

By: _____
Jae Hee Choi, Reg. No. 45,288
(858) 651-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

METHOD FOR NEGOTIATING WEAKENED KEYS IN ENCRYPTION SYSTEMS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. Application Serial No. 10/389,364, filed on March 14, 2003, which is a continuation ~~and claims the benefit~~ of U.S. Patent Application Serial No. 09/216,348, filed December 18, 1998, which are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

[0002] The present invention relates to the encryption of wireless communication signals, and relates in particular to the communication between systems having different encryption requirements. It has become commonplace to transmit messages, in the form of digital data, via wireless communication systems and/or the Internet.

[0003] Two general types of cryptography are secret key cryptography and public key cryptography. In the case of secret key cryptography, a message, often referred to as "plaintext", to be transmitted from a sender to an intended recipient is encrypted using a secret key and the intended recipient decrypts the encrypted message, frequently referred to as a "ciphertext" or a "cryptogram", using the same secret key. Only the secret key may be used to encrypt and decrypt the message and attempts made to decrypt the message with other keys will fail. A widely used secret key system is the Data Encryption Standard (DES) which employs a 56 bit key and 8 non-key parity bits. DES was published as a U.S. Federal Information Processing Standard in 1977.

[0004] The present invention is directed essentially to secret key cryptography.

[0005] The degree of security provided by a given encryption system depends on the strength, or work factor, of the system, which is commonly measured in terms of the number of bits in the key.

[0006] A work factor is a number, expressed in bits, which is the logarithm to base 2 of the maximum number of basic decryption operations which must be performed, using different trial keys, to determine with certainty which trial key corresponds to the actual key that was used for encryption. For example, the DES Algorithm has a work factor of 56 bits because it provides a key with 2^{56} possible values. As is known in the art, any trial key may be the correct key. Therefore, the correct key will usually be found after fewer than 2^{56} trials. On average, the correct key will be found after half of the possible trial key values have been tested. However,